WHOIS History Lookup: 3 Types of Domain Names to Avoid for the Sake of Cybersecurity

Posted on June 18, 2020

Expanding one's business online footprint with the right domain names should not just be left to business decision-makers, but also involve cybersecurity experts. Though old domains can bring benefits to the table, no enterprise wants to end up with those having a sinister past. WHOIS history queries via solutions such as WHOIS History Lookup, Search (from the Domain Research Suite), or API can help avoid that.

How so? Digging into a domain's WHOIS history allows you to gather more context about its past ownership, including whether it may have belonged to threat actors at some point and should therefore require greater scrutiny.

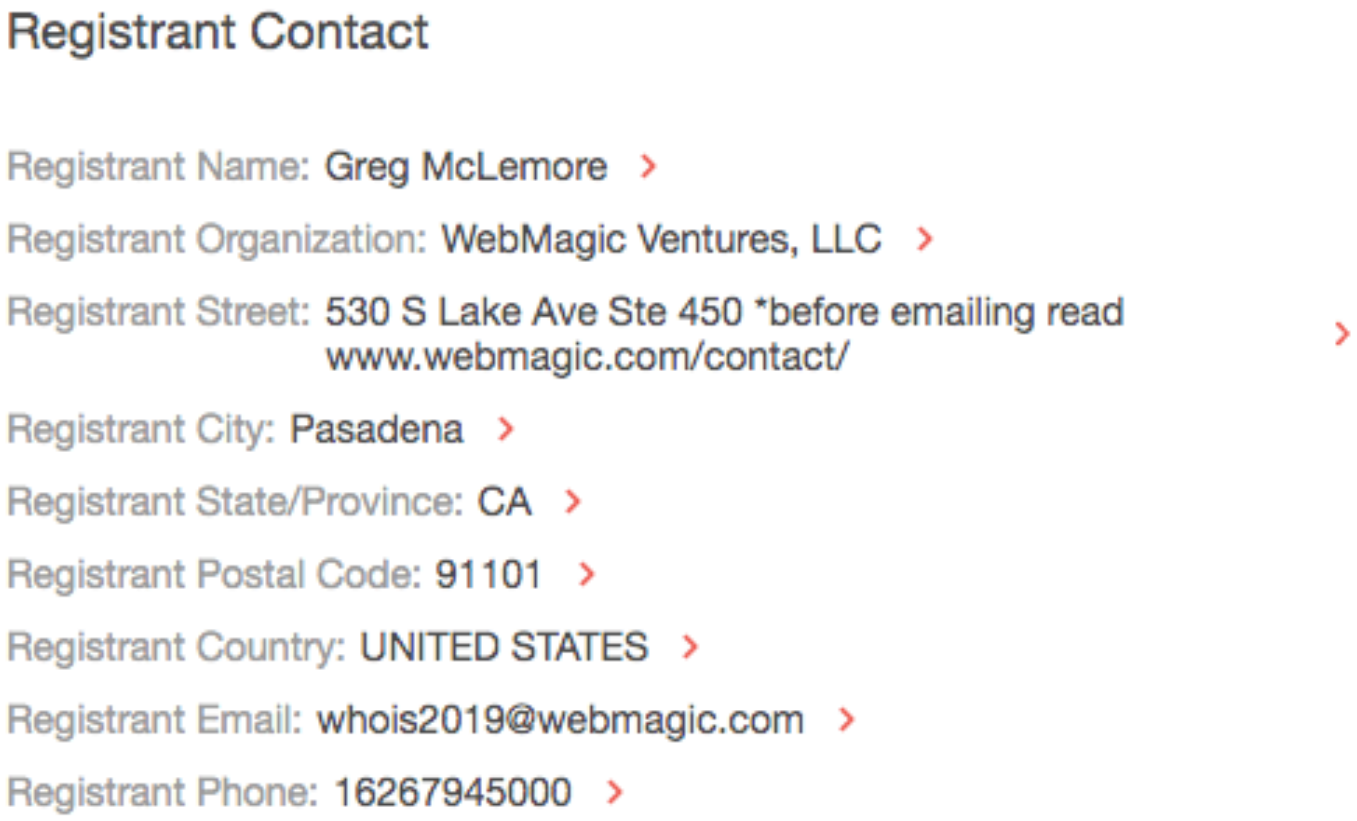
We compiled a list of domain history no-nos that can put a strain on your ventures' success (possibly landing your website on blacklists) or even cause harm to whoever might get into contact with them.

1. Avoid Domains Tied to Phishing

Phishing may be an age-old threat but it still accounts for 80% of reported security incidents. And since most phishing attacks begin with an email, we can often learn about phishers via the address's domain they used to send malicious messages.

Say, for instance, that you received an email address sporting account[.]com as a domain name. Alternatively, you may also be interested in buying this domain name because it's short and could be a nice addition to your product lines.

A WHOIS History Search query can tell you not only a domain's current registrant but also its past owners throughout its existence. For our sample, we found that account[.]com currently belongs to an individual, whose ownership wouldn't expire until July 2020. Thus, if you're interested in obtaining the domain, it would sound right to start negotiating for it. Assuming the owner is willing to part with it, however, due diligence suggests that you check if it has ties to any kind of malicious activity before the actual purchase.



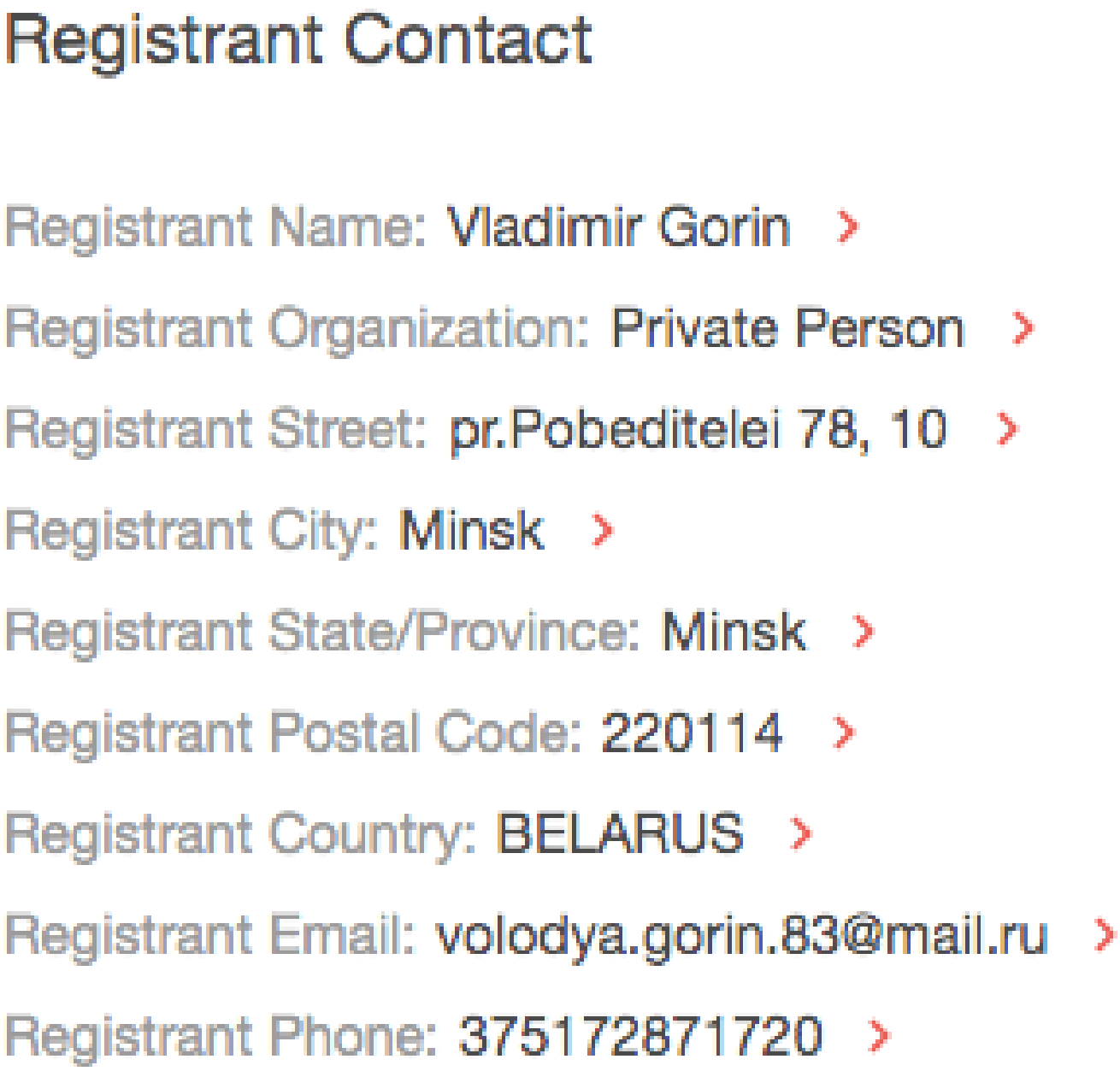
You can do a Web search for it. We discovered that variations of the domain commonly figuring in phishing attacks, such as one targeting PayPal. We verified this via the Threat Intelligence Platform (TIP) and discovered that account[.]com is indeed considered a malware host, according to PhishTank. Knowing that, it may still be on a blacklist, which means some potential consumers may never be able to access it.

2. Stay Away from Domains Connected to Malicious Organizations

Some cybercriminal gangs operate like established legitimate companies would. One example of this is the group behind the GozNym malware, which stole millions of dollars from several victims,

primarily businesses and financial institutions in the U.S., between October 2015 and December 2016.

Let’s say that you’re interested in adding the domain fabrics-for-life[.]com to your textile manufacturing division’s web portfolio. The first step to ensure that it’s not connected to a notorious organization is by running it through a domain history lookup. Domains that figure in attacks are normally included in various security solution blacklists and so could remain inaccessible to their users no matter how much time passes. Our query revealed that a Vladimir Gorin owned the domain up until 25 March 2016.



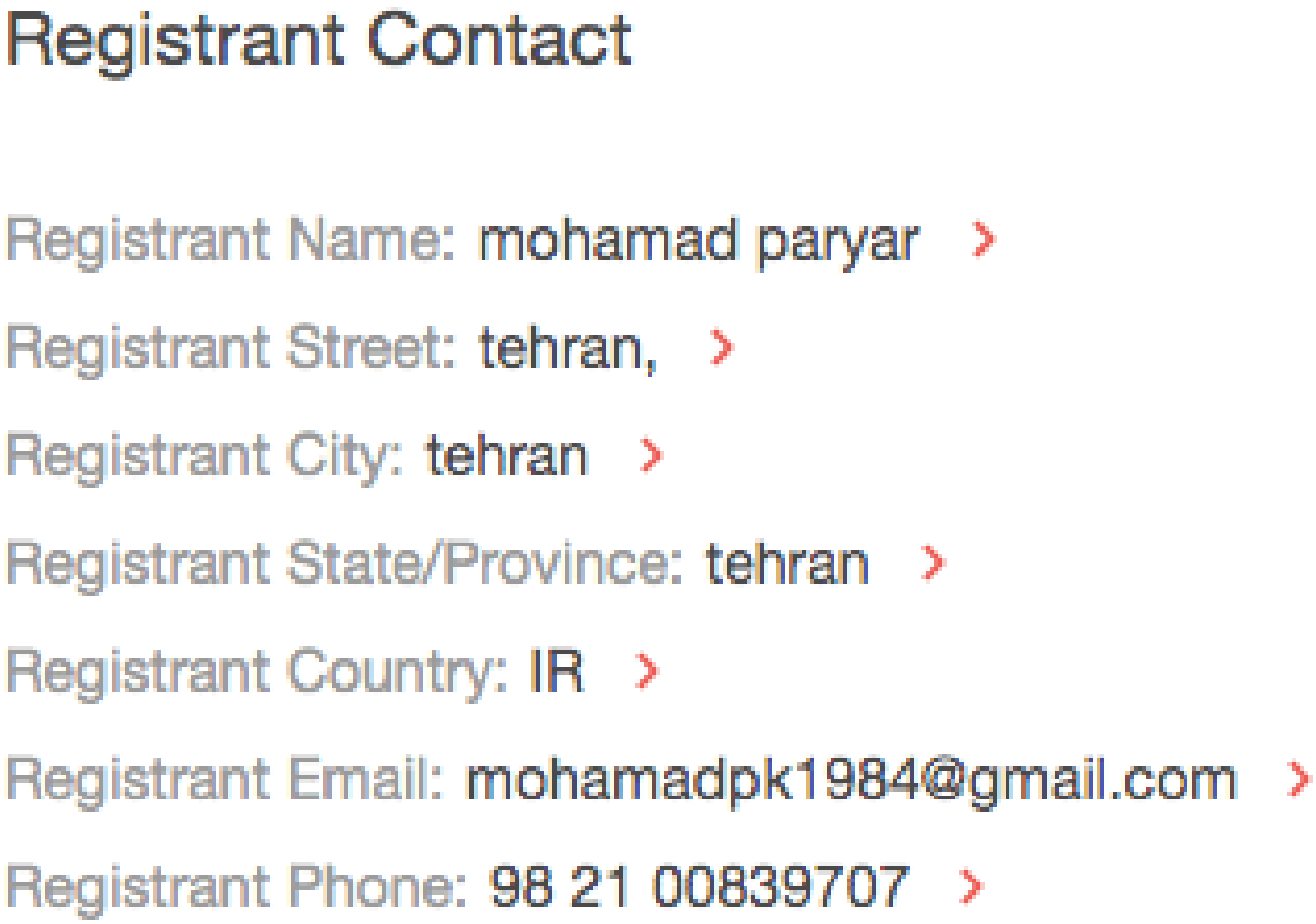
From the GozNym FBI page, you can see that one of the GozNym gang's members shares the name "Vladimir Gorin." That said, while fabrics-for-life[.]com may have been a perfect fit for one of your websites' home, it may not be a good idea to use it as it still may be part of security solution

providers' blacklists, making it unavailable to potential visitors.

3. Steer Clear of Domains Preowned by a Convicted Felon

You wouldn't want to purchase or interact with a domain formerly owned by a known cybercriminal either. For would-be purchasers, that domain may have been or is still being blocked by security solutions and even Internet service providers (ISPs) and search engines. And for security reasons, you don't want to become another of its victims.

So let's say that you were alerted to the domain pcmac[.]ir by your firewall and aren't sure how to deal with it. A WHOIS History Search can tell you that the domain has had a single owner (Mohamad Paryar) since its initial registration on 18 November 2017. By this time, you still have no idea why pcmac[.]ir was flagged. A potential reason could be its owner.



You can find out more about the domain's registrant via a Web search. You're likely to find an FBI wanted page for an individual with the same name as the top result. Knowing that, purchasing or interacting with the domain pcmac[.]ir doesn't sound like a good idea. Also, it may be safer to block all access to it if it does turn out to have ties to a convicted cybercriminal.

Domain history lookups using solutions such as WHOIS History Lookup, Search, or API are excellent means to learn more about a domain's past—be it to avoid interactions with dangerous online properties or secure a worthy domain name for business expansion.